IRJEAS
NURTURING RESEARCH

INTERNATIONAL RESEARCH JOURNAL
OF
ENGINEERING & APPLIED SCIENCES

ISSN: 2322-0821(0)
ISSN: 2394-9910(P)
VOLUME 10 ISSUE 3
Jul 2022 - Sep 2022
www.irjeas.org

Review Article

A Taxonomy of Security and Research Challenges in Cloud Computing

*Umang Garg [1], Neha Gupta[2], Mahesh Manchanda [3]

[1]Assistant Professor, Graphic Era Hill University, Dehradun, Uttarakhand, India
umangarg@gmail.com https://orcid.org/0000-0002-1815-5794
[2]Research Scholar, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
neha.judger99@gmail.com
[3]Asscociate Professor, Graphic Era Hill University, Dehradun, Uttarakhand, India
manchandamahesh@gmail.com https://orcid.org/0000-0002-9056-8999

**Corresponding Author* - umangarg@gmail.com

https://doi.org/10.55083/irjeas.2022.v10i03002

Received: 30 April 2022; Accepted: 08 July 2022

Abstract: Cloud computing is delivered as a storage service by third party. It gains wide acceptance from various Business organizations & Information Technology (IT) Industries. Cloud computing provides various services to users through the internet; those services are like Applications, computation, and storage etc. In spite of these advantages, cloud technology faces different types of privacy and security related issues. These issues become major barriers to adopt cloud technology into various organizations. This survey paper addresses the cloud architecture, various security and privacy issues, challenges and threats, attacks, and future research directions to overcome the security and privacy related problems in the cloud environment.

Keywords: Attacks, Cloud Architecture, Cloud Computing, Cloud Services, Privacy, Privacy Issues and Challenges, Security, Security Issues, Threats

1. INTRODUCTION

The evolution of cloud computing delivered through the following stages: initially creation of the network, sharing network, sharing information, sharing the resource, and service sharing. Cloud computing is mainly evolving from distributed computing. The main motivation of the distributed computing system is, to share the resources and utilize them in a better way. In distributed computing, the resource copy is shared between different users in the pay per use basis [1]. Cloud computing offers a virtualization technology. Virtualization is a technique, which is used to convert many physical computing devices into one or more virtual devices. Virtualization provides various benefits like scalability, availability, manageability and reduces the cost to the cloud users. The rest of the paper is sorted out into different sections. Section I presents the introduction; section II presents the history of cloud computing; section III presents a literature review of cloud computing. In section IV presents cloud architecture and basic concepts of cloud computing; section V discussed, the general cloud data security, various threats and attacks. Whereas section VI provides different types of cloud computing security issues; section VII discussed various cloud data storage privacy Issues and challenges. Section VIII concludes the paper with contributions, and finally, section IX presents the direction for future research.

2. HISTORY OF CLOUD COMPUTING

In 1961, the computer scientist John McCarthy introduced the basic concept of computing in a "cloud". In the year 1966 “Douglas Parkhill” explore the characteristics of cloud computing. Basically, the term "cloud" is evolving from telecommunication. In the telecommunication domain, firms started to offer VPN (Virtual Private Network) facilities to the user at very less cost. Before the evolution of VPN, telecom companies provide the services to the user by using committed point-to-point data circuits. The fundamental weakness of point-to-point information circuits is wastage of system data transfer capacity. To maintain a strategic distance from arranging data transfer capacity related issues VPN benefit was actualized. The telecom organizations by utilizing VPN administrations, using the general system data transfer capacity in a powerful way and adjusting the system movement. The cloud innovation utilizes VPN administration to interface distinctive data centers and system foundation all through the world [2]. In the mid-1990's "System Cloud" or "Cloud" was presented all through the systems administration industry. In the late 1990s, Salesforce.com started to carry remotely provisioned administrations into the venture.

In 2002, Amazon Web Services (AWS) stage was propelled by Amazon.com, which gives different ventures related administrations that remotely provisioned processing assets and business functionalities. The expression "distributed computing" was started in the business field from the year 2006. Amid this year, Amazon propelled its Elastic Compute Cloud (EC2) administrations; Google Apps likewise started giving program based venture applications [3].

3. LITERATURE SURVEY

In the paper [4], author exhibits a study of security problems as far as security risks and their remediation’s play out a parametric correlation of the risks being looked by cloud stages and think about different interruption recognition and counteractive action systems being utilized to address security risks. In the paper [5], authors proposed an outline of the security issues, existing arrangements and different distributed computing dangers for various variables, digital legal sciences apparatuses, and method, and security worries in private cloud suppliers. To give better security administration the creator recommends 3-level security design. In the paper [6], the author proposed different assaults in light of cloud parts and countermeasures for those assaults, in this paper, the author gives a relative investigation of the principle of interruption discovery/counteractive action frameworks and different security issues happened in the following ages. In Paper [7] writer give a low-down examination of the circulated processing issues and problems relating to security, with a focus on the figuring forms and the organization transport composes. This paper consists; the maker proposed distinctive security issues and troubles occurred in the cloud movement and game plan models. “Addressing security of cloud computing issues”, the purpose of this paper is evaluating cloud security by perceiving novel security necessities and to show a functional game plan that discards these potential threats [8]. In paper [9], highlights circulated processing building measures, conveyed registering key security essentials, disseminated figuring security risks and dispersed figuring attacks on security with their easing methodology, and research challenges in future [9].

In the paper [10], the author elaborates on various clouds computing, security issues, dangers, and their answers. In the paper [11], the different parts of distributed computing in regards to information lifecycle and its security and privacy challenges alongside the concocted philosophy to address those difficulties. We specify a portion of the controls and law prerequisites set up to guarantee cloud client information privacy. The author of the work [12] offers a broad diagram of security risks for numerous variables that influence distributed computing. Aside from that, a detailed discussion of a few major themes relating to the insertion framework, application, stockpiling framework, bunching difficulties, and so on.

4. ARCHITECTURE AND BASIC CONCEPTS OF CLOUD COMPUTING

The cloud design basically separated into two areas; the front end session and the back end session. The two segments are associated through the web. The front end area is valuable for clients interface with the cloud, while the back end session is the cloud framework. The back end session gives different administrations like PCs, servers, and information stockpiling to the clients.

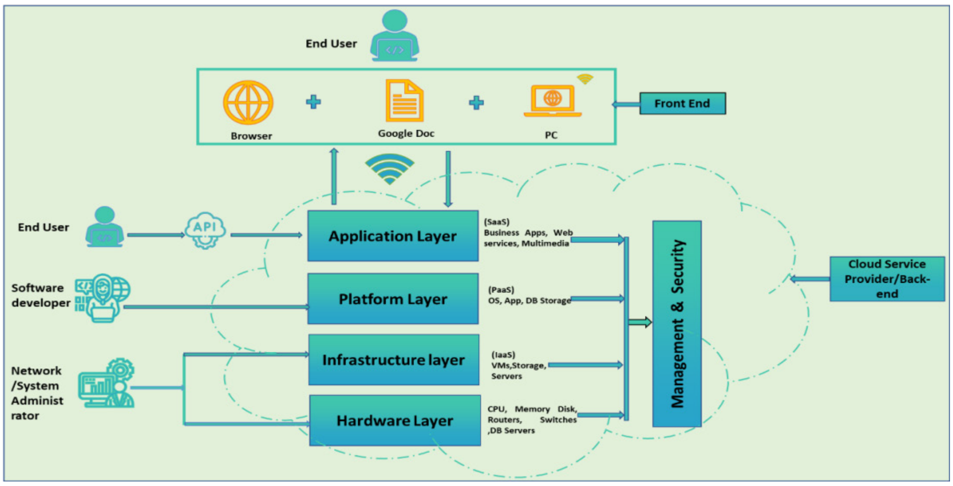
End User
Browser
Google Doc
PC
Front End
End User
API
Software developer
Network /System Administ rator
Application Layer
Platform Layer
Infrastructure layer
Hardware Layer
(SaaS) Business Apps, Web services, Multimedia
(PaaS) OS, App, DB Storage
(IaaS) VMs,Storage, Servers
CPU, Memory Disk, Routers, Switches ,DB Servers
Management & Security
Cloud Service Provider/Back-end

Figure 1- Cloud Computing Architecture

In the cloud condition of observing of activity, gets the client asks for and dealing with the cloud assets are finished by utilizing the focal server (central database server). The central database server takes after specific tenets and directions. The central database server utilizes Middleware programming for observing and dealing with cloud assets. Middleware gives connection organized PCs to speak with each other. The cloud computing architecture provides a different delivery model, deployment model, basic components, cloud security concepts and essential characteristics to the users ([3], [4]). Fig 1 shows the architecture of cloud computing.

Cloud Computing Delivery Model

In the cloud, the delivery model provides various types of computing services to the users those are:

A. Software as a Service (SaaS)

SaaS provides various applications and tools that are remotely maintained by different service providers. These applications are available to the customers based on their request, over the internet. In this model, the service providers provide the services to the customers in a pay-per-use manner.

SaaS provides various software applications, by using this facility the users directly access those applications and tools without installing on their PCs. In this model, the end users do not have any control to manage the cloud computing resources.

B. Platform as a Service (PaaS)

PaaS provides various platforms to the users for developing applications, running the applications and perform a testing operation on various applications. Developers develop their own applications based on the requirement of a specific platform without worry about fundamental backend infrastructure. PaaS providing platform layer resources to the customers in the rental basis over the Internet, these platform layer resources include different operating systems and various software frameworks.

The cloud users can access developed applications from anywhere through the internet. This model provides various advantages to the users, by using this model the users develop their individual applications without set up any product, stage or apparatuses in their PCs.

C. Infrastructure as a Service (IaaS)

IaaS offers various computing assets to the users as a service. Instead of vending physical hardware infrastructure, it offers virtualized infrastructure as a service. This model provides virtualization resources (storage, communication, and computation) to the users based on user request.

In IaaS, the user has control over the networking components like a host firewall, storage, operating systems and deployed applications in the cloud environment [5]. The service provider maintains these resources. The clients normally utilize the resources and pay the bill based on the usage of cloud resources. Compare to other delivery models in this model the user have great control over the cloud environment.

D. Anything as a Service (AaaS)

Anything as a Service is additionally called X as a Service where X might be everything as an administrator. This administration winds up indistinguishable in cloud view. The cloud framework can give diverse clients necessities utilizing Storage-as-a-Service, Integration-as-a-Service, and reduce the cost in staff, equipment, and physical space [5].

Cloud Deployment Models

In cloud architecture, deployment model consists of different models those are:

A. Public Cloud

In public cloud computing, the service provider makes resources available to consumers via web applications or web services over the Internet. By using the public cloud the number of users accesses the resources without having any constraints on cloud data. In public cloud security, related issues are very high compared to all other cloud models [19].

B. Private Cloud

In the private cloud are maintained and operated by a single organization or different cloud providers (third parties) as per their business requirement. In private clouds, all the resources are arranged inside a firewall.

The resources in Private clouds are accessed by only single organization people or specific users only. These are more secure than all other types of cloud models. Compare to other models, private cloud maintenance cost is high [20].

C. Community Cloud

The community cloud is a shared infrastructure model. The community cloud model was developing by combining different organizations, which follow the same rules and regulations. In a community cloud, all the resources are equally shared between different organizations people within the cloud. Compare to public cloud security more in a community cloud. This shared environment reduces costs compared to a private cloud [20].

D. Hybrid Cloud

It was constructed by different types of clouds (private, community, public) and makes a single cloud environment. Therefore, the hybrid cloud may offer standardized services to the general public at one end and propriety services to the single organization at the other end. Compare to the public cloud, the hybrid cloud provides more security to the cloud resources [8].

E. Virtual Private Cloud

The virtual private cloud also called as a hosted cloud. In this model, pools of shared resources allocated to users based on their demand. The virtual private clouds are hosted and managed by the public cloud provider and made available to various cloud customers [3].

Cloud Basic Components

Cloud components play a crucial role to provide various services to cloud users through the internet. The major cloud components are:

A. Virtualization

Virtualization assumes a key part in arranging a cloud environment. It is the key part of the cloud. It gives different figuring assets to various clients by making a virtual example of physical processing assets [5].

B. Multi-Tenancy

The multi-inhabitant condition can have different clients or clients can share their asset in an execution environment but does not see each other's data, even if they may not belong to the same organization [22].

C. Cloud Storage

Cloud storage is a storage unit, whenever the user wants to store or access data from the cloud it provides the services. Cloud storage is given by the cloud supplier, which is kept up, overseen, and moved down remotely and it made accessible over the system to the diverse clients [27].

D. The Hypervisor

The hypervisor also called a Virtual Machine Monitor (VMM).VMM permits running distinctive Virtual Machines (VM) on a solitary physical equipment framework. The real part of hypervisor is to deal with the different VMs, which are kept running on the physical or host framework.

E. Cloud Network

Cloud system can work on distinctive server farms; every datum focus contains a number of servers. To give security to server farms, cloud utilizing secure system set up called cloud organizes. Cloud organizes enables diverse clients to safely get to the assets from the cloud [21].

Cloud Computing Security Concept

In a cloud computing environment, to provide security in both distributed and multitenant environment become a challenging task. The client-server architecture facing lots of problems for securely transfer the data between service providers and users. In a cloud environment, the major security concerns are:

A. Software Security

The awareness of software security rises from engineer software department; it functions properly under various malicious actions. It's one of the challenges that comes up when working in a cloud environment.It defects with security containing various bugs and attacks [5].

B. Infra-Structure Security

In a cloud environment, the most essential challenge is to secure the virtual and physical infrastructure from various attacks and threats.

In the cloud condition specialist co-op or outsider, the individual gives the essential security to cloud foundations, yet it isn't adequate for preparing the basic business. So, organizations must keep up their own particular infrastructure security to have the capacity to approve business prerequisites more secure [5].

C. Storage Security

The storage system in a cloud environment is critical for storing end users' data in cloud storage areas or data centres. The security of end-user data stored in cloud data centres is crucial.The information proprietors don't have any thought, where the real information is found? It is an imperative component of giving Quality of Service (QoS) [5].

D.Network Security

Network security is the strength of cloud infrastructure. In cloud computing, communication between the server and the end user can be possible via the internet. In cloud environment network security attacks are occurred internally or externally either in virtual networks or physical networks [5].

Cloud Computing Actors

Based on the activity conducted by the persons/actors, the cloud computing environment is divided into five types:

A. Cloud Consumer (CC)

A person who accesses the resources from the cloud service provider/broker called as cloud consumer or end user. The cloud consumer maintains a business relationship with cloud service provider/broker and utilizes the resources provided by the cloud service provider.

B. Cloud Provider (CP)

A person or organization responsible for making services that are available to the end user called a cloud service provider.

C. Cloud Broker

A person acts as a mediator cloud broker is a middleman between a cloud service provider and a customer. Cloud broker negotiates the direct relation between provider and consumer.

D. Cloud Carrier

A mediator who gives network and transport of cloud administrations from CP to CC [23].

Characteristics of Cloud Computing

Cloud provides various characteristics those are:

A. Pools of Resource

In cloud computing condition asset pooling is accomplished through multi-occupant engineering. In a multitenant environment, multiple user's access pooled resources provided by the service provider.

B.Rapid Elasticity

In a cloud environment, rapid elasticity is achieved by quickly adding or removing computing resources like storage, processing, service, and tools based on user requirement.

C. Broad Network Access

In a cloud environment provide broad network access to cloud users. The data owners storing their personal information in the cloud server, this information can access from anywhere through the internet.

D.Measured Service

Cloud proved measured service to the users based on their usage of cloud data. Each user pays the amount based on their data usage. The amount of data usage measure and control by both data user and service provider sides [13].

E. On-Demand Self Service

The cloud provides various services to the user based on users request, the cloud provider provide the computing services to the user based on demand. The users use those services through the internet and pay the bill for using the data from cloud [13].

Advantages of Cloud Computing A.Easy Management

There are distinguished services in terms of hardware and software, Cloud computing is very powerful tool for end-user. The cloud administrator can easily handle all these computing resources very fewer efforts. The administrator can easily elaborate or reduce the storage space, computer resources based on user demand. At the user end, without installing applications on user pc directly access the resources or applications from the cloud through the internet [2].

B.Cost Reduction

Most of the IT/ business organizations, instead of maintaining own infrastructure for running a business, cloud provide rental or lease bases infrastructure for running the business. The cloud users by using this facility improve their business without installing the own infrastructure get the profit with less cost [2].

C.Uninterrupted Services

Cloud computing provides various computing services to the various user without having any interruption; the provider provides uninterrupted services to the user based on their demand [2].

D.Disaster Management

In cloud data centers, in case of any disasters occurs we can easily manage that disaster by maintaining the offsite backup facility. Most of the organizations keeping their confidential data in cloud data centers, if any disaster occurs, the total business go downstage. So keeping crucial data backups using cloud data centers is the need for most of the organizations [2].

E.Green Computing

Now a day, every organization using a number of a computer system for developing their business growth rate, due to the wide use of systems in organizations, harmful emissions, electronic waste, and energy consumption become higher. This can be reduced to some extent by using cloud computing services. This leads to develop the green computing and reduce the e-waste generated by the computer system in an organization [2].

Cloud Computing Challenges

Cloud computing provides various benefits to the users apart from that cloud faces various challenges, these challenges become a major barrier for developing cloud computing. Due to this reason many of the organizations fear to join the cloud. The major cloud computing challenges are as follow:

A.Security and Privacy

Security and privacy become a major barrier for adaption of cloud computing. Cloud provides pools of resources and multi-tenancy features to the user, these features are introduced new security and privacy challenges. The wellknown security and privacy issues are data losses, phishing, and access control [24].

B.Performance and Bandwidth Cost

Cloud gives different figuring assets to the client regarding equipment and software's, associations can spare some cash using equipment however they have to spend more cash on the system data transmission. For successful delivery of data in the cloud, it required sufficient bandwidth, if bandwidth is a high performance also high if bandwidth low the performance also decrease. For the small applications the required bandwidth less and cost may be small, but for the large applications required bandwidth more the cost was high [25].

5. SECURITY ISSUES IN CLOUD COMPUTING

Nowadays, data security and privacy issues related to a cloud environment are addressed in various kinds of literature [23]. These issues are occurred due to the lack of data integrity, confidentiality, availability, authentication, data authorization, non-repudiation, and data privacy. Fig 2 shows different cloud computing security and privacy principles.

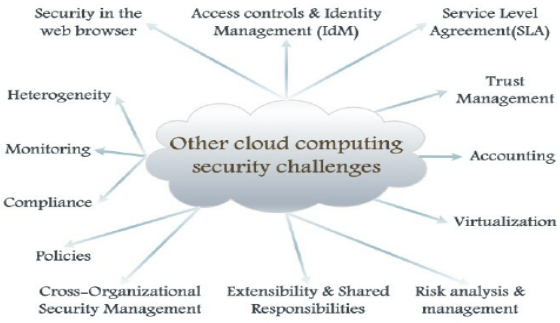
Security in the web browser
Access controls & Identity Management (IdM)
Service Level Agreement(SLA)
Heterogeneity
Trust Management
Monitoring
Other cloud computing security challenges
Accounting
Compliance
Virtualization
Policies
Cross-Organizational Security Management
Extensibility & Shared Responsibilities
Risk analysis & management

Figure 2- Principals of Cloud Service Security and Privacy

A. Data Integrity

Information trustworthiness is one of the imperative components in any data framework to give security. Information honesty implies shielding information from unapproved alteration and erasures or harms [16]. The data ought not to be changed amid the exchange of information amongst sender and collector. If the data is modified during transfer state, such type of attack is called modification. Modification attacks are occurring due to a lack of data integrity. Data integrity can be obtained by using various methods like message hashing technique, digital signature, and message authentication [23].

B. Data Confidentiality

Data confidentiality states that only intended recipient should able to access the information [16]. If any unauthorized users access that information, then data confidentiality gets compromised. As a result, data secrecy is the most critical feature of cloud security. Interception assaults due to a lack of confidentiality have happened [24].

C. Data Availability

Data availability means at any time the data should be available to authorized users [16]. If any disasters occur to the cloud data centers even though the data can be avail to the authorized users by using data backups provided by cloud administrators. If data is not available business-related issues may arise [26].

D. Data Authentication

Authentication assists to provide the proof of user identity. There are many ways to authenticate the user's data, those are, biometric mechanism and certificate verification [15]. Certificate verification provides more security compared to other security authentication mechanisms. Lack of proper authentication fabrication attacks is occurred [26].

E. Data Authorization/ Access Control

It confirms that the user is authorized to access specific information or not. Access control determines the people who access which type of data, up to which level [27].

F. Data Non- repudiation

If the sender sends any message to the particular data center or any recipient it is not possible to disagree the message was sent by the sender, this is called non- repudiation. [15].

G. Data Privacy

Privacy deals with the right of an individual or group of users control their personal or sensitive information themselves [16].

Security Threats in Cloud Computing

- Data Loss: - Data loss can be occurred due to data compromising, disaster management. Data can be compromised because of malicious attacks and natural disasters etc. [27].
- Information Breaches: - Data breach imply outflow of private information to unapproved clients. Information breaches can happen because of the absence of appropriate verification and approval strategies, review controls, inconsistent utilization of encryption keys, transfer challenges and working framework disappointment [21].
- Service Hijacking: - In this sort of issues, the unapproved client gets entrance control on login qualifications at that point bargained clients account [22].
- Information Collection: - Information can't be totally evacuated except if the gadget is crushed, aggressors can recover this information
- VM Jump: - VM jumps are happening, when a VM can get to another VM (that is, misusing hypervisor powerlessness)
- Revocation: - The mishap of the client plays out a bowed activity in a plan that does not have the adroitness to follow it. [5].
- Shared Technology Issues: - These problems will arise in multi-tenant systems, when numerous customers use a shared framework to supply on-demand services with the same virtual machine.
- Unknown Risk Profile: - Unknown risk profiles can coexist with major benefits such as time savings from maintaining the foundation and ownership transfer.
- Identity Theft: - When someone pretends to be someone else in order to get a client's credentials and benefits, this is known as identity theft.

Security Attacks In Cloud Computing

- Cross-Site Scripting (XSS) Attacks: These attacks occur when malicious code is inserted into a user's online page, diverting customers to the attacker's web page, and storing sensitive data.
- Domain Name System (DNS) Attacks: DNS attacks occur when a hacker is able to uncover vulnerabilities in the DNS to exploit.
- Man in the Middle (MITM) Attack: During the transmission of data between two parties, an unauthorised user gains access to the network and steals important information. The MITM attack's primary goal is to steal personal information [24].

- Denial of Service (DoS) Attacks: A denial of service (DoS) attack prevents legitimate users from accessing a resource, such as a website, network, or email, or makes it exceedingly slow. This type of assault is usually carried out by bombarding the target resource, such as a web server, with a large number of requests at once.

- Distributed Denial-of-Service (DDoS) Attack: - A distributed denial-of-service (DDoS) assault is one in which numerous compromised computer systems attack a target, such as a server, website, or other network resources, causing a denial of service for users of the targeted resource [25].

- Treat Poisoning: - In this type of attack, the treat's content is altered in order to get access to an unapproved programme or page. The treat contains sensitive accreditations concerning clients' information, and when the programmer accesses this content, he also has access to the content within these, allowing him to engage in illegal activities.

- Attack on Metadata Spoofing: - Metadata spoofing is a type of attack in which the attacker modifies the content of Web Services Description Language (WSDL) records in order to carry out unusual tasks for which she may not be permitted.

- Wrapping attack: - Wrapping assault is again another regular assault for online administrations and normally turns out to be exceedingly likely for cloud frameworks.

- Administration Infusion Assault: - Distractive administration entering through getting to benefit recognizable proof records, application and VM level assault.

- Malware Injection and Steganography Attacks: - In this attack, an attacker injected harmful code to the system applications or files during the transfer of data through the network.

- Shared Architectures: - On this attack, the attacker wontedly traces the execution path of a victim's application. By using this path an attacker to notice the victim's actions and steal his account.

I.

II.

6. CLOUD COMPUTING SECURITY

Security is the significant worries for IT project and business relations, the individuals who are thinking about receiving the cloud computing [11]. Cloud computing security issues are categorized into various kinds those are:

A. Embedded or Virtualization Security Issues

Virtualization is one of the accomplished affections provided by cloud. Virtualization plays an important role in the acceptance of cloud computing. In a cloud environment, due to virtualization users get added profits, but this affection faces a lot of security problems. The attackers try to carry out various attacks on the cloud, to damage the virtualization service. The major virtualization security issues are listed in the below table 1[25].

Table 1- Security Issues for Cloud Computing

Category	Security topic	Security issues
Embedded (or) Virtualization security issues	VM isolation	Data leakage, cross Virtual Machine attack
	Simple Network Management Protocol (SNMP) Server	The insecure setting, vendor patch
	VM monitoring,	Un-trusted hypervisor parts, the straightforwardness of hypervisor, the absence of a screen, hypervisor partition, VM escape, Load adjusting in the hypervisor.
	VM Programmability	VM bouncing, Cross-VM assault, Side- channel assault, Covert channel assault, Memory de-duplication issues, Malware infusion, Entropy age quality, Entropy consumption, VM reset issue, consistency, re-utilization, VM rollback.

• VM Isolation: Virtualization's core preferred viewpoint is one of limitation. One of the most basic challenges in cloud execution is workload disengagement among VMs. It has the potential to cause data leaks and crossVMs attacks. As a result, when delivering a virtual machine in the cloud framework, the disconnection method should be meticulously planned.

• SNMP Server (Simple Network Management Protocol): - It's a simple system administration standard intended as a low-cost component for collecting data from various devices.

- Virtual Machine Monitoring: In the virtual world, the host machine serves as a command centre for monitoring the applications of virtual machines. After everything is said and done, the screen will be exposed to all of the development data.

- VM Programmability: - For each programmable processor package in a cloud environment, business switches use pushed usefulness (e.g., accounting, blocking, and irregularity disclosure.) The most important test of using this device in an orchestrates processor is to run a package watching handiness for programming creation.

B. Trust, Compliance and Legal Aspects Issues

In the cloud accretion environment, trust is a non-measurable attribute that plays a significant impact. Assurance is the crucial agency in the cloud business environment that sits between the service provider and the customer. Assurance is suited for a wide range of arrangement-related systems. The SLA certificate is critical in the cloud business strategy. It's advantageous for accoutrement accord amid chump and account provider. SLA certificate consists of a set of rules and regulation; both parties have to chase those rules and adjustment during the period of SLA agreement. The major trust, compliance, and legal aspects issues are listed in below table 2 [25].

Table 2- Cloud Computing Trust, Compliance, and Legal Aspects

Category	Security topic	Security issues
Trust, compliance and legal aspects	Trusted third party	Data location, termination, Reliability protection, service level agreement [5].
	Human factor	Login credential sharing, phishing.
	Forensic factor	Disclosure of data.
	Reputation	Customer behavior and reputation isolation.

- Trusted Third Party (TTP): There are several users related to the Cloud data and server cultivators may mistreat it. TTP can authorise, audit, and confirm the ordered data, as well as provide unwavering quality assurance against unapproved software engineers. The customer has no idea where the data is kept in general.

- Human Factor: - In order to illuminate the role of humans in cloud security, it must first be understood that humans are at the root of all problems and can also cope with a large number of them.

- Forensic Value: As the use of online system applications grows, so does the amount of advanced wrongdoing. In a group and framework, computerised legal sciences play a critical role. Advanced legal sciences are becoming more well-known and important in the investigation of cybercrime and computer-assisted misbehaviour. Significantly, there are major concerns in the areas of information seizure, information, information disclosure, and secret information trafficking.

- Credibility: - The rapid advancement of distributed computing has attracted a lot of attention. A few sensible virtual machines are introduced on a similar system in a distributed computing environment, and they have identical equipment. Notoriety disengagement is a concern because the client's actions and exercises influence one other. The administration was mishandled by one of the clients. Client conduct monitors and, in most cases, the clients of most organisations; yet, commercial interests and reputation may be jeopardised.

C. Cloud Data Storage Security Issues

In cloud accretion ambiance abstracts accumulator security issues become above barriers for acceptance into the cloud. In accretion, ambiance information plays an above role. The abstracts owners are not aware, are the abstracts is amid in cloud accumulator center most and what blazon of security mechanisms they chase for accoutrement security to the abstracts within cloud abstracts centers. The major cloud data storage security issues are listed in below table 3.

Table 3- Cloud Data Storage Security Issues

Category	Security topic	Security issues
Cloud	Data warehouse	Loss of control, information region, validation,

data storage security issues	Data Availability	DoS/DDoS assault, flooding assault,
	Cryptography	Poor key administration, flawed crypto calculation, cloud blackouts, multi-location
	Data Breaches	Cloud blackouts, multi-location.
	Integrity and confidentiality	Poor key administration, flawed crypto calculation,
	Malware and worm	De obscurity assault, concealed personality.

- Data Warehouse (DWH): Abstracts warehouses are capable of accommodating the organising and analysis of various user populations, as well as their security requirements. Security is a crucial claim for completing and maintaining DWH deployments. [26].

- Accessibility: The primary goal of the cloud service is to provide customers with a high level of accessibility. It focuses on the client's ability to go anywhere at any time. Accessibility eludes the product, information, and delivers equipment to qualified clients as a request. A multi-level design, which is supported by stack adjustments and executed sequentially on several servers, will approach an attack based on an arrangement. As a result of the system's flooding assault, there are certain scattered storage needs in accessibility property. Insider vengeance is also a significant issue for it.

- Breach of Personal Information: - When plate drive bites the dust without making any reinforcement, it's an outcome of meddling activity, and information disaster may occur. It's the loss of security and trust, as well as a direct impact on the SLA strategy.

- Cryptography: - Numerous conditions in cryptographic segments seem to crash and burn when the security exertion associated. In cloud cryptography associated with overcoming the escape provisos in security locales anyway same time, it has various challenges still yet to survive. The poor key organization, figuring adequacy, certain data is moreover extraordinary issues related to cloud cryptography.

- Integrity, Availability and Confidentiality Issues: - The three fundamental difficulties of distributed storage are confidentiality, integrity, and availability (CIA). We examine the issue identified with respectability and privacy. As we all know, the most essential component in a data framework is honesty, which protects information from unapproved adjustments, cancellations, or changes. When a security parameter is incorrectly defined or VMs and hypervisors are constructed incorrectly, a security risk arises.

- Worms and Malware: Brilliant cybercriminals utilise e-wrongdoing attacks to infuse malware into distributed storage, turning them into 'zombies,' with the purpose of infecting larger system servers' PCs, which are referred to as Botnets. Proficient is well aware that it contains sensitive and private information. It could be separated by an assailant's faulty accounting and metadata security execution.

D. Clustering Computing Security Issues

Cluster computing different types of computers, virtual machine, servers are connected loosely or tightly together work to make a cluster system. The cluster computing security issues are listed in the below table 4 [21].

Table 4- Clustering Computing Security Issues

Category	**Security topic**	**Security issues**
Clustering computing security issues	Physical cluster	DoS attack, brute force.
	Virtual cluster	Misconfiguration, overseeing firm-product

- Physical Cluster: - Pack progressive expansion needs bounteous VM, servers, dealt with PCs to recognize a best exchange speed affiliation, computational power, and monstrous gatherer restrain. In perspective of best information exchange limit affiliation, a case abstracts set to change all through the gathering, which would be wonderful to the adversary and it can advantage them for showering DoS ambush.

- Virtual Cluster: - It can be either concrete or fundamental device keeps running on the grouped working game plan on the previously mentioned solid hub. Misconfiguring and overseeing firm-product issue.

E. Issues with Internet and Service Security

The Internet is useful for transferring the information in the form of packets from the source system to destination system using transmission (wired or wireless) media; transfer the packets from through the transmission media in the form of raw bits. Internet consists of a number of nodes; by using these nodes data transfer from source to destination. Issues related to the internet and service are listed in the below table 5.

Table 5- Issues related to Services

Category	Security Area	Security issues
Internet and services related issues	Service availability	Bandwidth under provisioning, Direct/indirect DoS attack, HTTP stateless protocol, improper WSDL documents, XML injection, Session hijacking, Cookie theft, cookie poisoning.
	Web technologies	Open network perimeter, Firewalls limitation, and limited mobile connection Rooting and jail breaking.
	Web services	Malicious insiders & system admin, hardware tempering, URL guessing attack, Archaic static password, XML SAML wrapping attacks, Weak credential reset methods.
	Internet Protocols	Bandwidth under provisioning, Direct/indirect DoS attack, HTTP stateless protocol, Session hijacking, Cookie theft, cookie poisoning.

- Service Availability: - These days DoS strike is extraordinarily usually found in the affiliations. The server cultivate has endless data server and diverse resources. From this time forward, to help a considerable measure of framework development, it is required a genuine information exchange limit and framework security.

- Web Technologies: - Web-based agents are used to access the bulk of cloud applications and services (e.g. different web browser). Different harmful online links and websites are rapidly increasing in the web environment; as a result of these web links, the attacker attracts the user and performs various attacks.

- Web Services: - Information integrity is a major concern in the distributed state. In any event, the issue of information respectability may be comprehended in distributed computing because of the Service Oriented Architecture (SOA) methodology.

- Internet Protocols: - The web-based cloud environment using various protocols for communication on the Internet, due to these protocols attackers perform different network-based attacks.

F. Network-Based Security Issues

Network security has become a major barrier for adopting into the cloud computing. Many of the security problems occurred in network level because in the cloud environment network is available in dynamic nature. Different types of network related issues are addressed here, like Denial of service attacks, Man in the middle attacks, Session hijacking, Network bandwidth related issues, Routing and load balancing related issues, changing network protocol, firewall-related issues, login security threats, IP spoofing, sniffing attacks, and Rooting and jail breaking. The network-based security issues are listed in the below table 6.

Table 6- Issues related to Network Security

Category	Security Area	Security issues
Network security issues	Circumference security,	Open network perimeter, Firewalls limitation, and limited mobile connection.
	Mobile platforms	Vulnerabilities, Malware, and Rooting.

- Edge Security (Circumference Security): - Edge security in a cloud environment is both static and dynamic security controls. The dynamic system security is created using deal with security gadgets that are installed in sort out progression pushing toward the point and on the entrance. This security technique assumes that the structural setup is static; nonetheless, this is risky these days [24].

- Platforms for mobile devices: - Bringing Your Own Device (BYOD) might be risky for businesses at times. To get to the project applications, the association worker employs their own unique contraption. This concept is beneficial from a proficiency standpoint, but it introduces security risks.

G. Access Control Related Issues

Cloud computing having numerous clients; every client having their own particular access rights to get to the information from the cloud [23]. The major access control related issues are discussed in the below table 7.

Table 7- Cloud computing access control issues

Category	Security topic	Security issues
Access control issues	Entity authentication	Archaic static password, XML SAML wrapping attacks, Weak credential reset methods25].
	User credentials	MITM attack, replay attack, TCP hijacking, network root attacks [25].

- Entity Authentication: - Cloud requires an approval framework to achieve secure access to cloud applications. Weak affirmation frameworks make cloud strikes, for instance, creature power and word reference ambushes.

- User Credentials: - The organization cloud server can store all users' credentials for providing services. Based on the user credentials server identifies user's authentication. These servers can be put either inside the cloud provider affiliation or outside the affiliation using a firewall. In a considerable application customer organization, overhead is developing the grounds that there are incalculable and each time required including, deleting, changing, sanctioning and deactivating customer accounts.

H. Software Security Issues

In current circumstances, Software security is the real concern. People groups create shifts programming programs by utilizing distinctive programming dialect and their own particular thoughts. The engineer takes after the arrangement to manage and compel for taking care of the product programs [18].

Table 8- Cloud Computing Software Security Issues

Category	Security topic	Security Issues
Software security issues	Platforms and frameworks	Uncertain system calls, bad SDLC mechanism
	User front-end	Expose of frontend interface

- Platforms and Frameworks: - In this part, give a huge report in regards to PaaS. The PaaS gives a distribution concept stage to go in light of the cloud application and bolsters unmistakable dialects that are useful for working up the cloud application. Each stage having different security related issue like resource metering, sort out restraint issue, and safe string end.

- User Front-End: - A purchaser gets to the Infrastructure as a service and Software as a Service gain from the use of a standard user interface over the internet. The client front-end has capacities that oversee and screen the use of administrations. As indicated by client approval the interface might be changed.

7. DATA PRIVACY ISSUES AND CHALLENGES

A. Privacy

Data privacy refers to how a small piece of information should be handled in light of its virtual significance. We frequently apply the concept of data privacy to basic individual data, also known as personally identifiable data, in the digital age. For a company, data privacy extends beyond the personally identifiable information of its employees and customers[16]. Some authors [2, 16, 15] proposed a different framework by using the hybrid approach to mitigate privacy issues in the cloud platform, for providing user authentication, confidentiality, and integrity of transmitted data between users and cloud service providers to mitigate privacy and security issues.

C. Privacy Issues

In the cloud environment, based on the different cloud scenarios the privacy issues are categorized into four subcategories, those are:

i. How to provide control to the users over their data, when the data is stored in the cloud environment and how to avoid the attacks from various attacks and unauthorized access.

ii. How to provide a guarantee to the user's data, where storing the duplicate data in different server locations and how to avoid data leakage, data loss, data breaks, and unauthorized data modifications.

iii. What level is the cloud subcontractors involved in data processing, checking, and ascertained?

iv. Who will take responsibility for providing legal requirements to the user's personal data? [15, 25].

C. Privacy Challenges in Cloud Computing

The best fundamental difficulties in cloud computing identified with privacy are:

1) The dauntlessness and intricacy of extensive hazard examination and appraisal of the cloud condition 2) New plans of action are continually developing which contrarily influences the privacy of cloud clients 3) Conforming to correlated laws and bearings [2].

8. CONCLUSION

Cloud computing provides various services to users through the internet on-demand basis. Many of the organizations moving their sensitive data towards cloud computing.

In cloud computing environment security and privacy plays a very crucial role, due to some unauthorized access, internal and external attacks cloud security and privacy become major barriers to achieving success in the cloud. There are numerous concerns about cloud security and privacy. This proposed article will provide ideas for researchers and developers on current cloud technologies, hype, and issues. This paper discusses the current state of security and privacy in the cloud system [22].

REFERENCES

[1] Ashish Singh, Kakali Chatterjee, "Cloud security issues and challenges: a survey" Journal of Network and Computer Applications, 2016.

[2] Atulkahathe, "Cryptography and network security" 3rd ed. Tata McGraw-Hill Education, 2013.

[3] Ayman M. El-Zoghby, "Cloud computing privacy issues, challenges, and solutions". 978-1-5386-11913/17, IEEE, 2017.

[4] Chao-Chih Chen, Lihua Yuan, Albert Greenberg. "Routing-as-a-Service (RaaS): A Framework for TenantDirected Route Control in Data Center", IEEE/ACM transactions on networking, vol. 22, no. 5, October 2014.

[5] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing." IEEE, 2012.

[6] Dimitrios Zissis∗, DimitriosLekkas, "Addressing cloud computing security issues" doi:10.1016/j. future. 2010.12.006.

[7] Dr.Arockiam L1, Parthasarathy G2, and Monikandan S3, "Privacy in cloud computing: a survey". CS & IT-CSCP 2012, pp. 321–330.

[8] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing".2017.

[9] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez., "An analysis of security issues for cloud computing." Journal of Internet Services and Applications 2013.

[10] Kresimir Popovic, Zeljko Hocenski, "Cloud computing security issues and challenges". IEEE Xplore, 2016.

[11] Kuyoro S, Ibikunle F., Awodele O., "Cloud Computing Security Issues and Challenges". IEEE Explore, 2016.

[12] Lahar Singh Nishad, Akriti, and Jaya Paliwal., "Security, Privacy Issues and challenges In Cloud Computing: A Survey". 978-1-4503-3962-9/16/03, ICTCS'2016.

[13] MariemBouchaala, Cherif Ghazel, Leila AzouzSaidane, Farouk Kamoun, "End to End Cloud Computing Architecture Based on A Novel Classification of Security Issues".2161-5330/17, IEEE, 2017.

[14] MaryemBerrezzouq, AbdellatifElghazi, "Issues and threats of data stored in the cloud. "978-0-7695-46476/12, IEEE, 2012.

[15] Minhaj Ahmad Khan, "A Survey of security issues for cloud computing". Journal of Network and Computer Applications, 2016.

[16] Mohammed Hussain, Hanady Abdulsalam, "SECaaS: Security as a Service for Cloud-based Applications", 978-1- 4503-0793-2, ACM, 2011.

[17] Mohsin Nazir, Mirza Shuja Rashid, "Security Threats with Associated Mitigation Techniques in Cloud Computing". International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868, Volume 5– No.7, May 2013.

[18] Naseer Amara, Huang Zhiqui, Awais Ali, "Cloud Computing Security Threats and Attacks with their Mitigation Techniques". 978-1-5386-2209-4/17, IEEE, 2017.

[19] Raj Kumar Buyya, James Broberg, Andrzej M. Goscinski, “Cloud computing principals and paradigms”, Wiley Press, New York, USA 2009.

[20] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal, “Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities.”978-0-7695-3352-0/08, IEEE, 2008, p.5.

[21] Saurabh Singh, Young-SikJeong, Jong Hyukpark. “A Survey on Cloud Computing Security: Issues, Threats, and Solutions”.Journal of Network and Computer Applications, 2016.

[22] SrijitaBasu, Arjun Bardhan, Koyal Gupta, PayelSaha et al, “Cloud computing security challenges & solutions-A survey”. 978-1-5386-4649-6/18, IEEE, 2018.

[23] Terzo, Pietro Ruiu, “Data as a Service (DaaS) for Sharing and Processing of Large Data Collections in the Cloud”.978-0-7695-4992-7/13, IEEE, 2013, p.475.

[24] Y Z Anet al, “Reviews on Security Issues and Challenges in Cloud Computing”. IOP Conf. Ser.: Mater. Sci. Eng. 160 012106, 2016.

[25] Yashpalsinh Jadeja, “Cloud Computing - Concepts, Architecture and Challenges”. 978-1-4673-0210-4112, IEEE, 2012, p. 877.

[26] Yuhong Liu*, Yan (Lindsay) Sun, JungwooRyoo and Syed Rizvi, Athanasios V. Vasilakos, “A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions”. Journal of Computing Science and Engineering, Vol. 9, No. 3, September 2015, pp. 119-133.

[27] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangzhou, "Data Security and privacy in cloud computing”, International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages.

Conflict of Interest Statement: *The authors declare that there is no conflict of interest regarding the publication of this paper.*